## REMARKS/ARGUMENTS

In the Office Action, the Examiner noted that claims 1-57 are pending in the application. The Examiner additionally stated that claims 1-57 are rejected. By this amendment, claims 10, 30, and 36 have been cancelled and claims 1, 11, 15, 22-25, 28-29, 31, 37-38, 40, and 46-51 have been amended. Hence, claims 1-9, 11-29, 31-35, and 37-57 are pending in the application.

Applicant hereby requests further examination and reconsideration of the application, in view of the foregoing amendments.

### In the Specification

Applicant has amended the specification to secure a substantial correspondence between the claims amended herein and the remainder of the specification. No new matter is presented.

### In the Claims

#### Claim Objections

The Examiner objected to claims 47-49 under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim, The Examiner required Applicant to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s). in independent form.

More specifically, the Examiner noted that claims 47-49 recite the apparatus as recited in claim 40, but that claim 40 is an independent claim that recites a method.

By this communication, Applicant amends claims 47-49 to recite the method as recited in claim 40, thereby placing the claims in proper dependent form. Accordingly, Applicant respectfully requests that the examiner withdraw the objections to claims 47-49.

#### Rejections Under 35 U.S.C. §102(e)

The Examiner rejected claims 1-57 under 35 U.S.C. 102(b) as being anticipated by Hashimoto, et al., US 6,k983,374 (hereinafter, Hashimoto). Applicant respectfully traverses the Examiner's rejections.

Regarding claim 1, the Examiner noted that Hashimoto discloses an apparatus for performing cryptographic operations, comprising:

- a cryptographic instruction, received by a computing device as part of an instruction flow executing on said computing device, wherein said cryptographic instruction prescribes one of the cryptographic operations; and (col.10, lines 37-60 and co1.28, lines 34-42)
- execution logic, operatively coupled to said cryptographic instruction, configured to execute said one of the cryptographic operations, wherein said one of the cryptographic operations comprises: (co1.5, lines 58-67 and col. 10, lines 5-8)
    - indicating whether said one of the cryptographic operations has been interrupted by an interrupting event. (co1.6, lines 1-18 and col.12, lines 52- 55 and col.13, lines 16-20; The Examiner asserted that Hashimoto discloses the execution of the program is often interrupted by an exception (or interruption) processing of the processor caused by the input/output or the like (co1.9, lines 38-40 and co1.27, lines 29-31), and thus, Hashimoto reads on the claimed interrupting event).

Applicant respectfully disagrees with the Examiner's characterization of Hashimoto and the rejection of claim 1. Applicant notes that Hashimoto's invention is directed toward the secure execution of an application program with has been encrypted in memory (Fig. 2, 2203) and for which an encrypted key (Fig. 2, 2205) is provided at a location keyaddr. Hashimoto teaches an instruction (execcenc keyaddr) which directs his processor to decrypt the encrypted key at keyaddr and which stores the key in a secret key register (Fig. 1, 2115). The contents of the secret key register 2115 are subsequently used to decrypt instructions of the encrypted application program which have been fetched from memory 2103 via a BIU 2118. The decrypted instructions are stored in an instruction buffer 2113 and are executed by an instruction execution unit 2112.

Hashimoto teaches provisions for the execution of an application program which has not been encrypted (i.e., "plaintext program"), and also for protecting the context information of an encrypted application program which is interrupted. (See, for example, col. 16,

lines23-40. Clearly, Hashimoto's invention is provided to protect an application program (and corresponding context information) from tampering.

But what Hashimoto does not teach, and which is provided for by the present invention, as recited in claim 1, is a cryptography unit, configured execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by a control word that is provided to said cryptography unit, and wherein said plurality of input text blocks are retrieved from memory, and wherein said plurality of output text blocks are stored to said memory. In other words, the present invention offers a programmer the ability to provide input text blocks in memory and to direct a computing device, via a cryptographic instruction, to perform cryptographic rounds on the input text blocks to generate corresponding output text blocks, which are stored to memory.

Hashimoto's teachings are limited to the execution of encrypted application programs and do not address general purpose cryptography, as is taught in the instant application. In fact, according to the present invention, any type of data may be stored in memory as input text blocks (e.g., data or program instructions), and the computing device be directed via the cryptographic instruction to either encrypt or decrypt the input text blocks. The corresponding output text blocks are then stored to memory.

Accordingly, it is requested that the rejection of claim 1 be withdrawn.

With respect to claims 2-9 and 11-29, these claims depend from claim 1 and add further limitations that are neither anticipated nor made obvious by Hashimoto. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 2-9 and 11-29.

By this amendment, claims 10 and 30 have been cancelled, thereby rendering the Examiner's rejections moot.

As per claim 31, the Examiner stated that Hashimoto teaches the apparatus for performing cryptographic operations, comprising:

- a cryptography unit within a device, configured to execute one of the cryptographic operations responsive to receipt of a cryptographic instruction within an instruction flow that prescribes said one of the cryptographic operations; and (col. 10, lines 37-60 and co1.28, lines 34-42)

- a bit within a register (co1.26, lines 58-60 and co1.27, lines 59-62), operatively coupled to said cryptography unit, configured to indicate that execution of said one of the cryptographic operations has been interrupted an interrupting event. (co1.6, lines 1-18 and co1.12, lines 52-55 and col.13, lines 16-20; noting that Hashimoto discloses the execution of the program is often interrupted by an exception (or interruption) processing of the processor caused by the input/output or the like (co1.9, lines 38-40 and co1.27, lines a 29-31), and thus, Hashimoto reads on the claimed interrupting event).

In reply, Applicant notes that, like claim 1, claim 31 recites a cryptography unit within a device, configured to execute one of the cryptographic operations responsive to receipt of a cryptographic instruction within an instruction flow that prescribes said one of the cryptographic operations, and wherein said cryptography unit is configured execute a plurality of cryptographic rounds on each of a plurality of input data blocks to generate a corresponding each of a plurality of output data blocks, and wherein said plurality of input data blocks are retrieved from memory, and wherein said plurality of output data blocks are stored to said memory. And as asserted above, Applicant points out that Hashimoto does not teach a cryptographic instruction that directs a device to retrieve input data blocks from memory, to perform a plurality of cryptographic rounds on the retrieved input data blocks to generate a corresponding output data blocks, and to store the output data blocks to memory. This is because Hashimoto's invention is solely directed toward the tamper-proof execution of an encrypted application program and not toward the above noted aspects of the present invention.

To support execution of cryptographic operations on the plurality of input text blocks in the presence of interrupting events, claim 31 also recites block pointer logic, operatively coupled to said cryptography unit, configured to direct said device to modify pointers to

said plurality of input and output data blocks in memory to point to next input and output data blocks at the completion of said one of the cryptographic operations on a current input data block. Hashimoto does not teach or suggest such an element.

With respect to claims 31-35, and 37-39, these claims depend from claim 31 and add further limitations that are neither anticipated nor made obvious by Hashimoto. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 31-35 and 37-39.

By this amendment, claim 36 has been cancelled, thereby rendering the Examiner's rejection moot.

With respect to claim 40, the Examiner opined that Hashimoto discloses a method for performing cryptographic operations in a device, the method comprising:

- executing one of the cryptographic operations responsive to receiving a cryptographic instruction, wherein the cryptographic instruction prescribes the one of the cryptographic operations; and (col.10, lines 37-60 and col.28, lines 34-42)
- indicating whether an interrupting event has occurred during said executing. (col.6, lines 1-18 and col. 12, lines 52-55 and col. 13, lines 16-20; asserting that Hashimoto discloses the execution of the program is often interrupted by an exception (or interruption) processing of the processor caused by the input/output or the like (col.9, lines 38-40 and col.27, lines 29-31) and thus, Hashimoto reads on the claimed interrupting event).

Applicant respectfully disagrees and notes that amended claim 40 recites, among other elements and limitations:

- retrieving a plurality of input data blocks from memory;
- executing one of the cryptographic operations on the plurality of input data blocks to generate a corresponding plurality of output data blocks, wherein said executing is performed responsive to receiving a cryptographic instruction, and

wherein the cryptographic instruction prescribes the one of the cryptographic operations; and

- storing the corresponding plurality of output data blocks to the memory.

As has been highlighted above in the traversals of the rejections of claims 1 and 31, Applicant respectfully points out that Hashimoto does not teach or otherwise disclose an instruction for use by a devices that directs the device to retrieve input data blocks from memory, to perform a specified cryptographic operation thereon to generate corresponding output data blocks, which are then stored to memory. Moreover, Hashimoto does not teach any apparatus or method which would provide for indicating that an interrupting event has occurred during the execution of the cryptographic operation, nor does he teach mechanisms (e.g., block pointer logic) for preservation of intermediate results when such interruptions occur.

Accordingly, it is requested that the rejection of claim 40 be withdrawn.

With respect to claims 41-57, these claims depend from claim 40 and add further limitations that are neither anticipated nor made obvious by Hashimoto. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 41-57.

## CONCLUSIONS

Applicant believes this to be a complete response to all of the issues raised in the instant office action and further submits, in view of the amendments and arguments advanced above, that claims 1-9, 11-29, 31-35, and 37-57 are in condition for allowance. Reconsideration of the rejections is requested, and allowance of the claims is solicited.

Applicant also notes that any amendments made by way of this response, and the observations contained herein, are made solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent business Goals (PBG), 65 Fed. Reg. 54603 (September 8, 2000), and are furthermore made without prejudice to Applicant under this or any other jurisdictions. It is moreover asserted that insofar as any subject matter might otherwise be regarded as having been abandoned or effectively disclaimed by virtue of amendments made herein and/or incorporated in attachments submitted with this response, Applicants wishes to reserve the right and hereby provides notice of intent to restore such subject matter and/or file a continuation application in respect thereof.

Applicant earnestly requests that the Examiner contact the undersigned practitioner by telephone if the Examiner has any questions or suggestions concerning this amendment, the application, or allowance of any claims thereof.

I hereby certify under 37 CFR 1.8 that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office on the date of signature shown below.

Respectfully submitted,

**HUFFMAN PATENT GROUP, LLC**

/Richard K. Huffman/

By: _____

**RICHARD K. HUFFMAN, P.E.**
Registration No. 41,082
Tel: (719) 575-9998

01/16/2001

Date: _____